CLAIMS

What is claimed is:

Sub a1

1. A method of examining a network, including:

identifying an operating system of a remote host, including a version and a patch level of the operating system;

identifying a service of the remote host, including a version and a patch level of the service; and

identifying a vulnerability of the network based on information obtained from the steps of identifying an operating system and identifying a service.

2. The method of claim 1, wherein:

the step of identifying an operating system includes sending a first set of packets to the remote host and receiving a second set of packets from the remote host in response to said first set of packets;

the step of identifying a service includes sending a third set of packets to the remote host and receiving a fourth set of packets from the remote host in response to said third set of packets, wherein information contained in said third set of packets is based on information received in said second set of packets;

the step of identifying a vulnerability includes comparing information contained in the second set of packets and the fourth set of packets to preexisting information in a database.

3. The method of claim 1, wherein the step of identifying an operating system includes sending three sets of packets to the remote host and receiving three respective sets of responsive packets from the remote host.

4. A method of examining a network, including:

nonintrusively and reliably identifying an operating system of a remote host including identifying a version of the operating system;

nonintrusively and reliably identifying a service of the remote host including identifying a version of the service.

5. The method of claim 4, further including:

identifying a vulnerability of the network.

6. The method of claim 4, further including:

identifying a trojan application on the host.

7. The method of claim 4, further including:

identifying unauthorized software use on the host.

8. The method of claim 4, further including:

identifying security policy violations on the network.

9. The method of claim 4, wherein:

the step of identifying an operating system further includes identifying a patch level of the operating system;

the step of identifying a service further includes identifying a patch level of the service.

10. The method of claim 4, wherein the steps of identifying an operating system and identifying a service each includes:

sending a selected packet to the remote host;

receiving from the remote host a reflexive responsive packet.

11. The method of claim 4, wherein the steps of identifying an operating system and identifying a service each includes:

sending a plurality of selected packets to the remote host;

receiving from the remote host a plurality of reflexive responsive packets.

12. The method of claim 4, wherein:

the step of identifying an operating system includes sending a first set of packets to the remote host and receiving a second set of packets from the remote host in response to said first set of packets;

the step of identifying a service includes sending a third set of packets to the remote host and receiving a fourth set of packets from the remote host in response to said third set of packets.

13. A method of examining a network, including:

identifying an operating system of a remote host including identifying a version of the operating system;

identifying a service of the remote host including identifying a version of the service; and

identifying a vulnerability of the network.

14. The method of claim 13, wherein:

the step of identifying a vulnerability includes using information obtained from the steps of identifying an operating system and identifying a service to identify the vulnerability.

15. The method of claim 13, wherein:

the step of identifying an operating system further includes identifying a patch level of the operating system;

the step of identifying a service includes identifying a patch level of the service.

16. The method of claim 13, wherein the steps of identifying an operating system, identifying a service, and identifying a vulnerability each includes:

sending a selected packet to the remote host;

receiving from the remote host a reflexive responsive packet.

17. The method of claim 13, wherein:

the step of identifying an operating system includes sending a first set of packets to the remote host and receiving a second set of packets from the remote host in response to said first set of packets;

the step of identifying a service includes sending a third set of packets to the remote host and receiving a fourth set of packets from the remote host in response to said third set of packets;

the step of identifying a vulnerability includes comparing information contained in the second set of packets and the fourth set of packets to information in a database.

18. The method of claim 17, wherein:

information contained in said third set of packets is based on information received in said second set of packets;

information contained in said fifth set of packets is based on information received in said fourth set of packets.

19. A method of examining a network, including:

sending a set of selected packets to a host on the network;

receiving from the remote host a set of reflexive responsive packets;

identifying conditions of the remote host by using information received in the reflexive responsive packets, wherein the conditions include an operating system of the host, and a service of the host.

20. The method of claim 19, wherein the conditions further include a vulnerability of the host.

21. The method of claim 19, wherein the conditions further include the presence of unauthorized software.

22. The method of claim 19, wherein the conditions include the presence of a trojan application.

23. The method of claim 19, wherein:

identifying an operating system includes identifying a version;

identifying a service includes identifying a version.

24. The method of claim 19, wherein:

identifying an operating system includes identifying a version and a patch level;

identifying a service includes identifying a version and a patch level.

25. The method of claim 19, wherein

the step of sending a set of selected packets to a host on the network includes sending a plurality of sets of packets to the host;

the step of receiving from the remote host a set of reflexive responsive packets includes receiving a like plurality of sets of reflexive responsive packets.

26. A method of detecting a vulnerability of a network, comprising:

sending a first set of selected packets to a host on the network;

receiving a second set of packets from the remote host in response to the first set of packets;

sending a third set of selected packets to a host on the network, wherein information contained in the third set of packets is based on information contained in the second set of packets;

receiving a fourth set of packets from the remote host in response to the third set of packets;

sending a fifth set of selected packets to a host on the network, wherein information contained in the fifth set of packets is based on information contained in the fourth set of packets;

receiving a sixth set of packets from the remote host in response to the fifth set of packets;

based on information contained in the second, fourth, and sixth set of packets, identifying an operating system of a host on the network, including a version and a patch level.

27. The method of claim 26, further including:

sending a seventh set of selected packets to a host on the network;

receiving an eighth set of packets from the remote host in response to the seventh set of packets;

sending a ninth set of selected packets to a host on the network;

receiving a tenth set of packets from the remote host in response to the ninth set of packets;

based on information contained in the eight and tenth sets of packets, identifying a service of a host on the network, including a version and a patch level.

28. The method of claim 27, further including:

based on information contained in at least the tenth sequence, identifying a vulnerability.

29. The method of claim 26, wherein:

the first set of packets includes:

a SYN Packet with false flag in the TCP option header;

a Fragmented UDP packet with malformed header (any header inconsistency is sufficient), where the packet is 8K in size;

a FIN Packets of a selected variable size or a FIN packet without the ACK or SYN flag properly set;

a generic, well-formed ICMP ECHO request packet;

the third set of packets includes:

a generic well-formed TCP Header set to 1024 bytes in size;

a Packet requesting an ICMP Timestamp;

a Packet with min/max segment size set to a selected variable value;

a UDP packet with the fragment bit set;

the fifth set of packets includes:

a TCP Packet with the header and options set incorrectly;

a well-formed ICMP Packet;

a Fragmented TCP or UDP packet;

a packet with an empty TCP window or a window set to zero;

a generic TCP Packet with 8K of random data;

a SYN Packet with ACK and RST flags set.

30. A method of examining a network, comprising:

sending a plurality of packets to a network;

receiving a responsive plurality of packets from the network;

comparing information in the responsive packets to information stored in a database;

based on the comparison, identifying a plurality of network conditions, including a vulnerability of the network.

31. A method of examining a network, comprising:

sending packets to a network;

receiving responsive packets from the network;

comparing information in the responsive packets to information stored in a database;

based on the comparison, identifying a trojan application on the network.

32. A method of examining a network, comprising:

sending packets to a network;

receiving responsive packets from the network;

comparing information in the responsive packets to information stored in a database;

based on the comparison, identifying unauthorized software use on the network.

33. A method of examining a network, comprising:

sending packets to a network;

receiving responsive packets from the network;

comparing information in the responsive packets to information stored in a database;

based on the comparison, inferring an unknown vulnerability.

34. A method of examining a network, comprising:

sending packets to a network;

receiving responsive packets from the network;

comparing information in the responsive packets to information stored in a database;

based on the comparison, identifying a security policy violation.

35. A system for examining a network, comprising:

a database including a set of reflex signatures;

a packet generator;

a comparison unit in communication with the packet generator and the database;

wherein the packet generator is designed to generate and transmit a plurality of test packets to the network;

wherein the comparison unit is designed to receive responsive packets from the network and to compare responsive packet information with the reflex signatures.

36. The system of claim 35, wherein the comparison unit is further designed to identify a vulnerability in the network based on its comparison of packet information with reflex signatures.

37. The system of claim 35, wherein the comparison unit is further designed to identify an operating system type, version, and patch level and a service type, version, and patch level of a host on the network.

38. The system of claim 35, wherein the comparison unit is designed to provide information to the packet generator, and wherein the packet generator is designed to use the information to selectively generate packets.

39. A computer readable medium, having instructions stored therein, which, when executed by a computer, causes the computer to perform the steps of:

identifying an operating system of a remote host, including a version of the operating system;

identifying a service on the port and a service of the remote host, including a version of the service; and

identifying a vulnerability of the network based on information obtained from the steps of identifying an operating system and identifying a service.

40. The computer readable medium of claim 39, wherein:

the instructions for identifying an operating system further include instructions for identifying a patch level of the operating system; and

the instructions for identifying a service further include instructions for identifying a patch level of the service.

41. The computer readable medium of claim 39, wherein:

the step of identifying an operating system includes sending a first set of packets to the remote host and receiving a second set of packets from the remote host in response to said first set of packets;

the step of identifying a service includes sending a third set of packets to the remote host and receiving a fourth set of packets from the remote host in response to said third set of packets, wherein information contained in said third set of packets is based on information received in said second set of packets;

the step of identifying a vulnerability includes comparing information contained in the second sequence of packets and the fourth sequence of packets to information in a database.

42. A method for use by a host on a network, comprising:

receiving a set of selected packets from remote equipment;

automatically sending a second set of packets to said remote equipment, which packets include information that enables the remote equipment to identify a vulnerability on the network.

43. A method for use by a host on a network, comprising:

receiving a first set of packets from remote equipment;

automatically sending a second set of packets to said remote equipment;

receiving a third set of packets from the remote equipment;

automatically sending a fourth set of packets to the remote equipment;

receiving a fifth set of packets from the remote equipment;

automatically sending a sixth set of packets from the remote equipment;

receiving a seventh set of packets from the remote equipment;

automatically sending an eighth set of packets from the remote equipment;

receiving a ninth set of packets from the remote equipment;

automatically sending a tenth set of packets from the remote equipment;

wherein said second, fourth, and sixth sets of packets include information that enables the remote equipment to identify an operating system on the network, including a version and a patch level;

wherein said eighth and tenth sets of packets include information that enables the remote equipment to identify a service, including a version and a patch level.